Commonwealth Office of Technology Monthly Cyber Security Tips

November 2007 Volume 2, Issue 11

Phishing

From the Desk of the Chief Information Security Officer

What is Phishing?

Phishing is a form of identity theft where the intent is to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information.

How Does It Work?

A phisher will send you an email or an instant message The message may appear to be from a friend, a business, a government agency or some other entity. Common phishing scams typically claim to be credit card companies, banks and major online retailers such as eBay, PayPal and Amazon. Some phishing attempts are easy to identify because they claim to come from businesses or companies that you have never dealt with; others may be more difficult to identify since they appear to be from entities with which you do business.

A phishing message may indicate that the entity had problems with their computers or data and that they simply need to verify your account information so you won't be inconvenienced the next time you try to use their services. Or the email message might be that there has been a suspicious purchase made by your credit card. If you did not make this purchase, you need to "contact us by using this link." Another example is a message claiming that you have just won the lottery, and if you would just go to this "secure" website and send them your bank account information, they'll put your winnings into your account. Another variation might be an email claiming to be from the IRS and due to an accounting error they just found, you have a refund. If you would just tell them your bank account number, they could process the refund.

Regardless of which story the phishers provide, they emulate a legitimate business or organization. The end result if you fall prey to phishing email may be unauthorized purchases using your credit card or emptying out your bank or other financial account.

What Should I Watch For To Determine if an Email is a Phishing Email or Not?

- Does the email ask you to "verify your information" or to "confirm your user-id and password"?

- Does the email reference any consequences should you not 'verify your information'?
- Most important, remember that legitimate businesses should never ask for personal or financial information via email.

How Can I Avoid Becoming a Victim?

- If it appears to be a phishing email, simply delete it. You can also forward it to the company it claims to be from and to spam@uce.gov.
- Do not click on any links listed in the email message and do not open any attachments contained in the email. Many phishing messages and sites not only attempt to get your personal information, they also attempt to install malicious code, like a Trojan horse, on to your computer.
- Do not enter personal information in a pop-up screen. Legitimate companies, agencies and organizations don't ask for personal information via pop-up screens.
- Install a phishing filter on your email application and also for your web browser. These filters will not keep out all phishing messages, but it will reduce the numbers of phishing attempts.

Anything else I should do?

- Review your credit card and bank statements or bills from the companies you do business with, looking for unauthorized charges or withdrawals.

For more information on phishing visit:

AntiPhishing Work Group: www.antiphishing.org/
i-Safe Phishing Video: http://ftc.isafe.org/phishing.html
OnGuard Online: www.onguardonline.gov/phishing.html
National Consumer League's Internet Fraud Watch: www.fraud.org/tips/internet/phishing.htm
US CERT: www.us-cert.gov/cas/tips/ST04-014.html

For more monthly tips visit:

www.msisac.org/awareness/news/

Brought to you by:

MS-ISAC
www.msisac.org

COT
http://technology.ky.gov